Chapter 1 Reliability Models

Introduction

In this chapter we will look at some of the most common methods of evaluation of reliability in safety systems.

In the last chapter we learned about generalized probability distribution functions (pdf) and cumulative distribution functions (CDF). In this chapter we will attach some meaning to these terms in the context of safety systems.

The pdf f(t) will be used to define the probability of failure of a system **at time *t*.** The CDF F(t) will be used to define the probability of failure over time period Δt.

Therefore the CDF $F(t) = \int_0^t f(t)dt$

Conversely the pdf $f(t) = \frac{dF(t)}{dt}$

As we shall see, definition of success and failure are important to construction of accurate models.

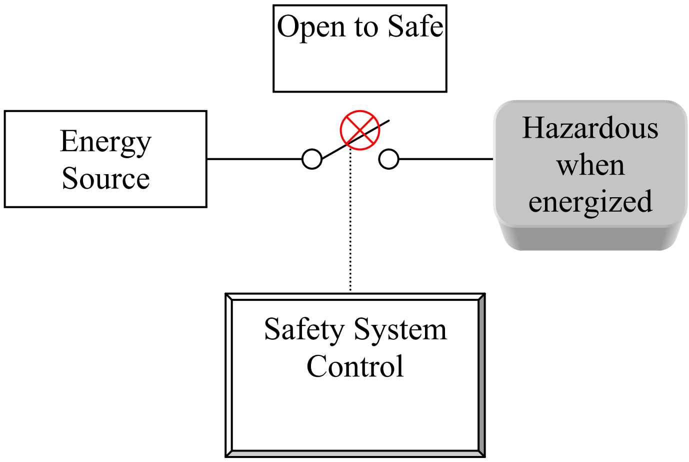
$$\begin{aligned} P(success) + P(failure) &= 1 \\ P(failure) &= 1 - P(success) \end{aligned} \tag{1.1}$$

In safety systems we are concerned with the probability of success, i.e. the probability that the system will work as intended, and the probability of failure, the probability that the system will not function at the time that there is a demand placed on the system.

Reliability R(t) – the probability that a system will operate over a designated time period. Unless otherwise noted, the starting time is 0.
R(t) = 1-F(t)
Reliability is the probability of success

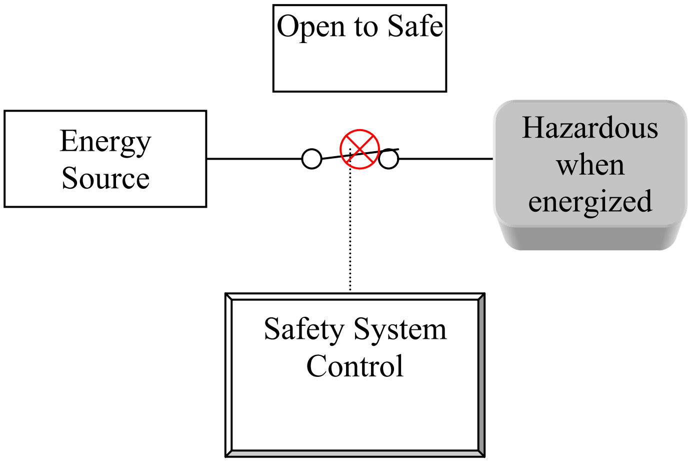
Unreliability F(t) =Probability of failure over a designated time period.
F(t)=1-R(t)
Unreliability is the probability of failure

In safety systems, F(t) is the probability that a system will fail during a designated mission time. In safety systems, the failure mode is very important. For example a switch that fails open, thus cutting off energy to a hazardous device, is failed but **failed-safe**. This type of failure is termed fail-to-safe.



Switch failed to safe.

Of greater concern is the switch that fails closed and is unable to transition to the open or safe state, even when commanded to do so by the safety system. This is termed **fail-to-danger** or **PFD**.



Switch failed dangerous.

Of the failure modes of the system, there is a subset of probabilities that a system will fail–to-safe (pfs) or fail-to-danger (pfd) at a given time t.

$$pfs(t) = f(t)_{safe} \tag{1.2}$$

$$pfd(t) = f(t)_{dangerous} \tag{1.3}$$

! Don’t confuse this with pdf=probability distribution function !

The complementary cumulative probability of safe or dangerous failure over time is the **PFD** and **PFS**. Note that it is the average PFD that is used in the definition of SIL levels for safety systems.

$$PFD(t) = F(t) - PFS(t) \tag{1.4}$$

Risk reduction factor RRF is the amount of risk mitigation required from the safety system. It is equal to 1/PFD$_{avg}$.

Failure Rate λ(t) (in some places called hazard rate): A measure of the instantaneous rate at which components fail.

$$\lambda(t) = \frac{f(t)}{1 - F(t)} = \frac{f(t)}{R(t)} \tag{1.5}$$

Note that items that are given as "rates per unit time" are sometimes just referred to as the "frequency" of the item. e.g λ(t) = failure rate or frequency of failure.

$$\lambda(t) = \frac{\#units\ \ failed\ over\ time\ t\ at\ time\ t}{Total\ \#units} \tag{1.6}$$

Note that λ(t) can be divided into safe failure rates and dangerous failure rates.

$$\lambda(t) = \lambda^D(t) + \lambda^S(t) \tag{1.7}$$

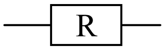
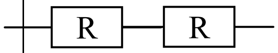
Mean Time to Failure (MTTF). By definition MTTF is the measure of the mean of a CDF with respect to time. The mean value of a probability function is given by

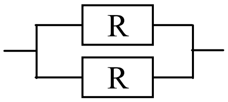
$$\hat{u} \cong \int_{-\infty}^{\infty} xf(x)dx \tag{1.8}$$

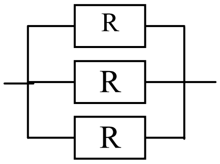
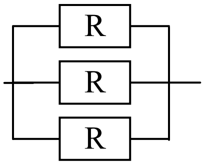
$$MTTF = \int_{0}^{\infty} R(t)dt \tag{1.9}$$

For a constant failure rate, the MTTF is the time that one would expect that 63.2% (1-e^{-1}) of a given number of components would have failed.

Availability A(t) – the probability that a system is successful at time t *assuming that a hazard can be present at time t.*

Configuration	Reliability for Constant Failure Rate λ(t)= λ	PFDavg Approximation	General System Reliability	MTTF (assumes repair time << MTTF)
Single  	$e^{-\lambda t}$	$\frac{\lambda^{DU} \cdot TI}{2}$	R_i	$\frac{1}{\lambda}$
Series  	$e^{-(\lambda_1+\lambda_2)t}$	$\frac{\lambda^{DU} \cdot TI}{2}$	$\prod_{i=1}^{n} R_i$	$\frac{1}{\sum_{i=1}^{n} \lambda_i}$

Parallel

 	
	$e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}$	$\frac{\left(\lambda^{DU} \cdot TI\right)^2}{3}$	$1-\prod_{i=1}^{n}(1-R_i)$	$\frac{1}{\lambda_1}+\frac{1}{\lambda_2}-\frac{1}{(\lambda_1+\lambda_2)}$
				if $\lambda_1=\lambda_2$ then
				MTTF=$\frac{3}{2\lambda}$

1/3 voting  	$3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$	$\frac{\left(\lambda^{DU} \cdot TI\right)^3}{4}$	$1-\prod_{i=1}^{n}(1-R_i)$	$\frac{11}{6\lambda}$
2/3 voting  	$3e^{-2\lambda t} - 2e^{-3\lambda t}$	$\left(\lambda^{DU} \cdot TI\right)^2$	$1-\sum_{i=0}^{m-1}\left(\frac{n}{i}\right)R^i(1-R)^{n-1}$	$\frac{5}{6\ \lambda}$
m/n voting	$\sum_{i=m}^{n}\binom{n}{i}e^{-i\lambda t}(1-e^{-\lambda t})^{n-1}$	$\frac{n!}{(m-1)!(n-m+1)!}\frac{\left(\lambda^{DU}TI\right)^{n-m+}}{(n-m+2}$	$1-\sum_{i=0}^{m-1}\left(\frac{n}{i}\right)R^i(1-R)^{n-1}$	$\frac{1}{\lambda}\sum_{i=m}^{n}\frac{1}{i},\ 1 \le m \le n$

1oo2 Redundancy

For a 1oo2 system:
PFD average is approximately (Goble pp 274)

$$PFDavg(t) = \frac{1}{TI}\int_0^{TI} (\lambda^D t')dt' \tag{1.10}$$

$$PFDavg = \frac{(\lambda^D \cdot TI)^2}{3} \tag{1.11}$$

If common cause failure modes are added
The full block diagram, including common cause and systematic errors is:

$$PFD_{avg} = \left[\left((1-\beta)\lambda^{DU}\right)^2 \frac{TI^2}{3}\right] + \left[(1-\beta)\lambda^{DU}\lambda^{DD}\cdot MTTR\cdot TI\right] + \left[\beta\lambda^{DU}\frac{TI}{2}\right] + \left[\lambda^D \frac{TI}{2}\right]$$

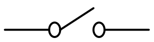
(1.12)

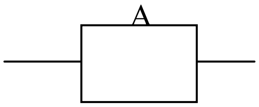
For the purposes of the models given in the next section:

Fail Safe
Open/Isolated/Unenergized

Fail Unsafe
Closed/Connected/Energized

1 **o**ut **o**f 1
1oo1



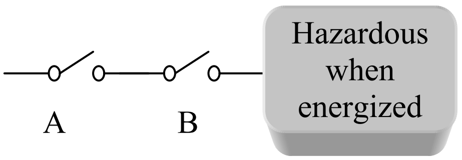


Success = A

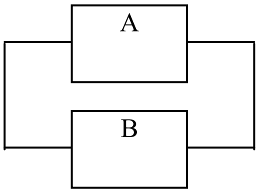
(1.13)

(1.14)

1oo2



Switch failed dangerous.



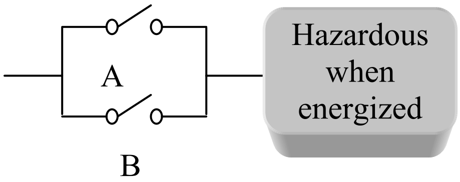
Success = A + B

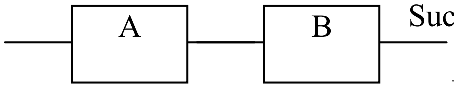
$$1-\prod_{i=1}^{n}(1-R_i)$$

$$MTTF_{1oo1} = \frac{1}{\lambda^S + \lambda^D}$$

In the redundant system above, success is defined as either switch A opening **OR** switch B opening.

2oo2



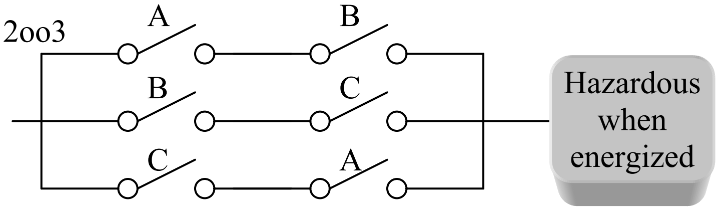


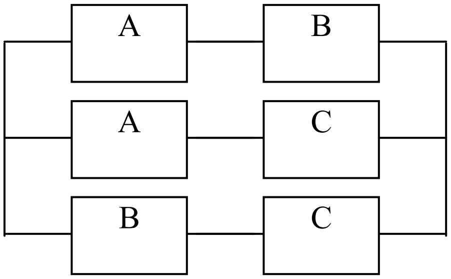
Success = A *B

$$\prod_{i=1}^{n} R_i$$

In the system above, success requires both switch A opening **AND** switch B opening. This type of configuration is not typical in accelerator safety systems.

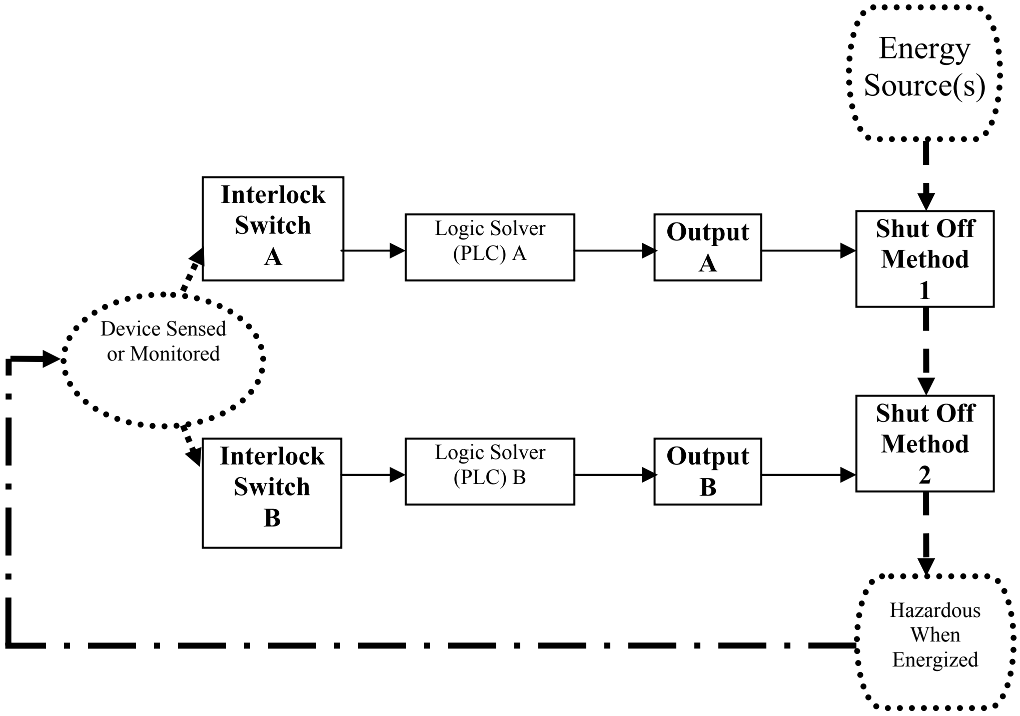
2oo3

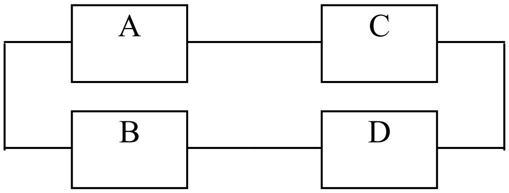




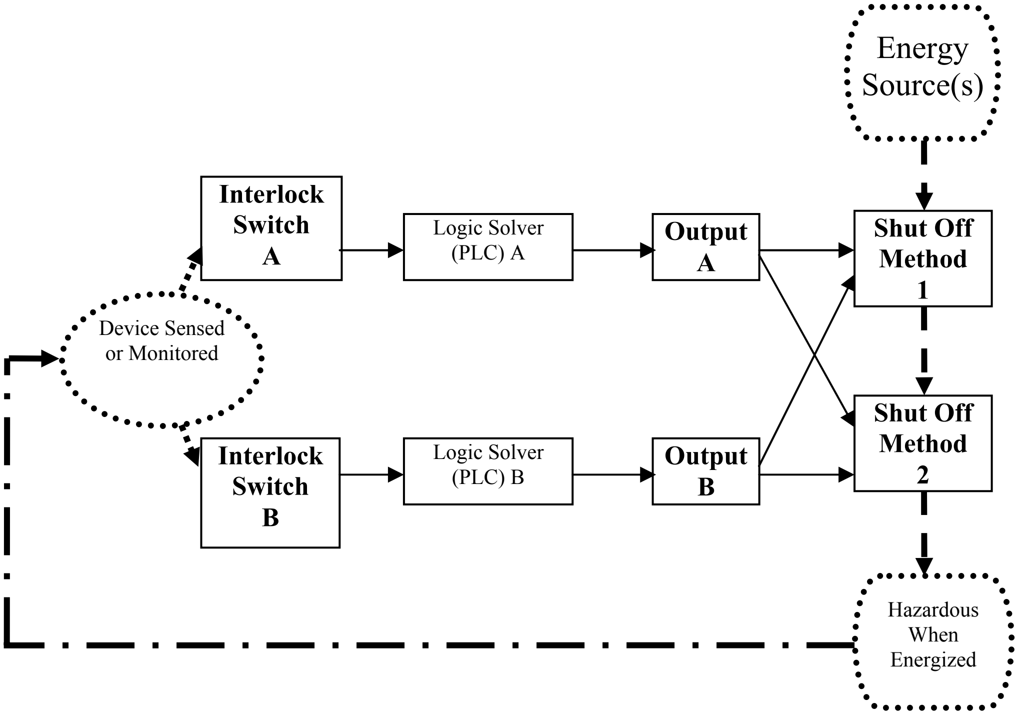
Control can be by:
Direct – direct shut off of energy source
Isolation- isolate energy source from hazardous location
Containment- keep hazardous energy within a barrier
Redirection – shunt energy to alternate, safe, location

Typical redundant safety system architecture





State	Combination	System Status
0	ABCD	OK
1	ABC~~D~~	OK
2	AB~~C~~D	OK
3	AB~~CD~~	Failed
4	A~~B~~CD	OK
5	A~~B~~C~~D~~	OK
6	A~~BC~~D	Failed
7	A~~BCD~~	Failed
8	~~A~~BCD	OK
9	~~A~~BC~~D~~	Failed
10	~~A~~B~~C~~D	OK
11	~~A~~B~~CD~~	Failed
12	~~AB~~CD	Failed
13	~~AB~~C~~D~~	Failed
14	~~ABC~~D	Failed
15	~~ABCD~~	Failed


Energy Source(s)
Interlock Switch A
Logic Solver (PLC) A
Output A
Shut Off Method 1
Device Sensed or Monitored
Interlock Switch B
Logic Solver (PLC) B
Output B
Shut Off Method 2
Hazardous When Energized